Annual Report to Congress on Foreign Economic Collection and Industrial Espionage

This report is was prepared by the National Counterintelligence Center.
For more copies of this report, please contact, Chief, Analysis Branch,
703-874-4018.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage

Key Findings

This annual examination by US government agencies of the threat of foreign economic collection and industrial espionage is conducted in compliance with Congressional mandate. Information obtained during the past year showed no reduction in attempts by foreign government, corporations, and individuals to acquire US proprietary economic information:

- The increasing value of trade secrets in the global and domestic marketplaces and the corresponding spread of technology with dual applications have contributed to a significant increase in both incentives and opportunities for economic espionage.

- Foreign counties continue to target items in all 18 categories of the Department of Defense Militarily Critical Technologies List. The most sought-after critical technology categories in 1999 in rank order were information systems, sensors, lasers, electronics, and aeronautic systems technologies.

- In addition to activities in the United States, foreign collectors also operate against US economic interests in their respective countries and in third countries. These activities conducted outside US territory are more difficult to identify and counter.

Reverse Blank

Contents

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage

Background

The Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359 requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the brochure *Foreign Economic Collection & Industrial Espionage Remains a Threat—Are You a Target, 1999.*

The Authorization Act specifies that these annual reports examine three aspects of the threat to US industry: the number and identity of the foreign governments believed to be conducting industrial espionage, the industrial sectors and types of information and technology targeted by such espionage, and the methods used to conduct espionage.

In coordinating a community-based response to the stated requirement, the National Counterintelligence Center (NACIC) requested the assistance of the Intelligence Community and the private sector. The following government components provided information for this report:

- Air Force Office of Special Investigations.
- Central Intelligence Agency (CIA).
- Defense Intelligence Agency (DIA).
- Defense Security Service.
- Department of the Army.
- Department of Energy (DOE).
- Department of State, including the Bureau of Intelligence and Research and the Bureau of Diplomatic Security.
- Federal Bureau of Investigation (FBI).
- National Reconnaissance Office.
- National Security Agency (NSA).
- Naval Criminal Investigative Service.
- US Customs Service.

In addition to information provided by the Intelligence Community, NACIC officers also interviewed a number of industrial security specialists from selected Fortune 500 companies, representing different sectors of the US economy.

There are no agreed upon definitions of economic or industrial espionage. For the purposes of this report NACIC will heed to the US Attorney General's definition of **economic espionage** as "the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies." This definition excludes the collection of open and legally available information that constitutes the overwhelming majority of economic collection. Aggressive intelligence collection that is entirely open and legal may harm US industry but is not espionage. This, however, can help a foreign intelligence service identify and fill information gaps, which in some cases may be a precursor to economic espionage.

Industrial espionage is defined as activity conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private US company for the purpose of obtaining commercial secrets. This definition does not extend to activity of private entities conducted without foreign government involvement, nor does it pertain to lawful efforts to obtain commercially useful information, such as information available on the Internet. Although some legal actions may be a precursor to clandestine collection, they do not constitute industrial espionage. Some countries have a long tradition of ties between government and industry; however, it is often not easy to determine what is foreign government-sponsored espionage, a necessary requirement under the Economic Espionage Act, Title 18 U.S.C., Section 1831.

Another term used in this report is **proprietary technology and economic information**, the definition of which is information not within the public domain and that which the owner has taken some measures to protect. Generally, such information concerns US business and economic resources, activities, research and development, policies, and critical technologies. Although it may be unclassified, the loss of this information could adversely affect the ability of the United States to compete in the world marketplace and could have a detrimental effect on the US economy, ultimately weakening national security. Commonly referred to as "trade secrets," this information typically is protected under both state and federal laws.

Overview of the Threat to US National Security

In a world that increasingly measures national power and security in economic as well as military terms, the United States continues to be threatened by the theft of proprietary economic information and critical technologies. The risks to sensitive business information and advanced technologies have dramatically increased in the post–Cold War era as foreign governments—both former adversaries and allies—have shifted their espionage resources away from military and political targets to commerce. The information they seek is not simply technological data but also financial and commercial information that will give their countries a competitive edge in the global economy.

During the past year, foreign governments, corporations, and individuals have continued to collect economic, technological, and trade secret information through a variety of legal and illegal means. The global spread of technology and the corresponding increase in the value of trade secrets have contributed to a significant increase in both the incentives and opportunities for conducting such activity. Much of what these foreign rivals (and allies) seek is in the public domain. Just as with traditional political-military espionage, however, trends in the collection of open-source information can be important indicators of strategic objectives that might ultimately be met by resorting to collection methods that are not legal. This report notes such trends.

Targeted US Defense Information and Technology

A review of reported suspected targeting incidents against critical technologies categorized in the Department of Defense (DoD) Militarily Critical Technologies List (MCTL), Part I: Weapons Systems Technologies in 1999 reaffirmed that all 18 categories of critical technologies continue to be the subject of foreign interest for military and economic exploitation. The 18 categories are, in order of suspected targeting: information systems; sensors and lasers; electronics; aeronautics; armaments and energetic materials; marine systems; guidance, navigation, and vehicle; signature control; space systems; materials; manufacturing and fabrication; information warfare; nuclear systems technology; power systems; chemical-biological systems; weapons effects and countermeasures; ground systems; and directed and kinetic energy systems. In 1999 as in 1998, foreign governments and commercially sponsored entities continued to target US companies involved in developing weapon components, new technologies, and technical information. Figure 1 illustrates the four categories with the highest percentage of reported targeting and the

Figure 1: Most Frequently Reported Targeted Technology [a]

Information Systems
HF, VHF military radios
Encryption devices (KYU-5, KG-84, KY-57)
Satellite communications (SATCOM) systems
Signal processing
Sensors and Lasers
Underwater acoustics
Infrared (IR) detectors
Airborne and ground radar
Imagery dissemination software
Digital terrain data
IR imagery
Optical night-vision products
Photonics
Thermal-imaging camera
Antisubmarine warfare and electro-optical sensors
Passive communications intercept and electronic intercept receivers
Electronics
Airborne switching and logic devices
Control units for missile launchers
Flight control systems for military drones
High voltage systems for night-vision goggles, tank sights, and rifle scopes
Hybrid electronic circuit amplifier used in radar jamming, Tempest/hardening of equipment, integrated circuits, transducers, semiconductors, and VHF/UHF SATCOM repeaters
Aeronautics Systems Technology
F-110/F-120 state-of-the-art engines
F-22 fighter planes
Chinook helicopter
Aerial gunnery target system
F/A-18 Hornet
C-130J
Engine safety systems for aircraft
Gas turbine engines
Brazing and welding techniques in aircraft manufacturing
R&D efforts in increasing engine efficiency

[a] (U) Technology headings are listed in rank order.

Attempt To Acquire Laser Gun Sights and Potassium Cyanide

On 30 September 1999, the Department of Commerce imposed a $10,000 civil penalty on Laser Devises, Inc., a Monterey, California, exporter, to settle allegations that the company attempted to illegally ship laser gun sights to Taiwan. Commerce alleged that in March 1995 Laser Devices attempted to export US-origin laser gun sights to Taiwan without the required Commerce authorizations.

On 30 September 1999, Commerce imposed a $5,000 civil penalty on Gilbert & Jones, Inc. of New Britain to settle allegations that the company exported potassium cyanide to Taiwan without the licenses required by the Export Administration Regulations. Commerce's Bureau of Export Administration alleged that on two occasions—one in 1994 and the other 1995—Gilbert & Jones, Inc., exported US-origin potassium cyanide to Taiwan without obtaining the required export licenses.

subcategories most often reported as being targeted in 1999. The DoD MCTL can be viewed on the Internet at www.dtic.mil/mctl/.

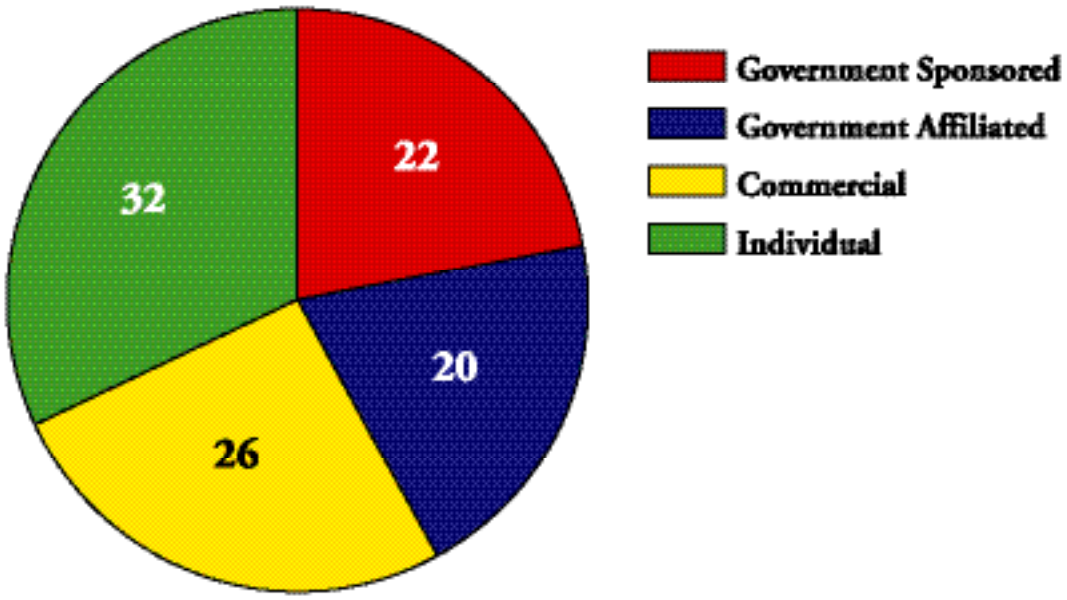
The extent of foreign interest in specific categories of technology varied dramatically from country to country. Contrary to private industry's belief, the leading-edge technologies are not the only technologies being targeted. Countries with less developed industrial sectors often prefer older "off-the-shelf" hardware and software. They will also seek military technologies that are at least a generation old because such technologies cost less, are easier to procure, and are more suitable for integration into their military structures.

More developed and traditional threat countries seem to seek technical information that will enable them to disable, copy, neutralize, or cause significant change to US military systems. By contrast, other countries often seek command, control, and decisionmaking systems, and information on major ground, airborne, and seaborne weapon systems, sometimes to enhance interoperability.

Figure 2 illustrates the origins and the associated percentages of the targeting. According to US defense industry reporting, targeting connected to commercial and individual foreign collectors accounted for 58 percent of the total suspicious activity. Government-sponsored targeting, including military and other official government activity, accounted for 22 percent of suspicious activities. Targeting activities by government-affiliated entities—including institutes, laboratories, and universities—accounted for another 20 percent.

The majority of the technology targeted in 1999 consisted of components rather than complete systems. This collection trend is associated with both developed and developing countries and seems to be driven by a requirement to upgrade existing platforms, rather than obtain new systems.

Figure 2: Percentage of Targeting



Collection Methods

Foreign collectors seldom use one method of collection; they combine collection techniques into a concerted effort that includes legal and illegal methods, while becoming more innovative in the new millennium. Specialized training and instruction courses in business intelligence collection methodology are becoming increasingly available. Such courses provide instruction on how to conduct HUMINT operations, including how to develop, create, and maintain dossiers and psychological profiles on potential sources; exploitation and elicitation techniques; debriefing methodologies; competitor targeting, including how to exploit industrial conventions, seminars and meetings; and real-world practical exercises.

In addition to traditional HUMINT recruiting strategies, studies of economic espionage consistently identify two primary techniques as the methods used to acquire economic intelligence:

• **Open-Source Collection**
- Requesting information through e-mail or letters.
- Exploiting Internet discussion groups.
- Exploiting multinational conferences, business information exchanges, or joint ventures.
- Misleading open-source collection.

• **Illegal Collection**
- Acquisition of export-controlled technologies.
- Theft of trade secrets, critical technologies, and critical information in host country.
- Agents recruitment, co-optees, and US volunteers.

Open-Source Collection

Requesting Information Through E-Mail or Letters. Request for information is the most often reported method of operation by foreign collectors to obtain trade secrets, critical technologies, and sensitive and classified information. The use of e-mail is the vehicle of choice to solicit information, and the use of e-mail is becoming more common in countries with limited or highly restricted public Internet access. However, use of postcards and letters for information requests continues.

The majority of the suspicious requests reported by industry are indirectly solicited. Requests can be linked to information available on Internet Web sites, in advertisements, in articles in trade journals, and in marketing materials at trade shows and seminars. The requests range from legitimate inquiries to those clearly seeking information that is restricted or sensitive. The inquiries may start as mundane solicitations for price lists, catalogues, published papers, research assistance, or for assistance in finding employment. Requests become suspicious when they originate from embargoed countries, pose questions that would reveal sensitive or classified information, or indicate that the requester is trying to evade export control or security procedures. Persistent requests from the same source also raises suspicion.

Company annual reports, patent data, corporate and government Internet sites, and marketing materials are exploited. Open-source research can inadvertently provide a collector with sensitive or restricted information, or assist in further targeting efforts by identifying industry and government relationships with specific technologies and activities. Many foreign collectors are technically astute and diligent readers of company publications; they attend industry conferences and trade shows; and they exploit professional contacts through memberships in trade and professional associations.

Highly assertive collection efforts are dubbed by some government agencies and private industry as aggressive open-source collection or AGGROS.

Exploiting Internet Discussion Groups. The anonymity of the Internet makes it a perfect medium for collection attempts using e-mail, search engines, and discussion groups. One technique is the exploitation of listserv, an e-mail-based discussion group organized along topics of interest and open to anyone. Subscribers who join a list may send an e-mail message to the list.The message in turn is sent to all members of the group by the listserv, which provides subscribers with e-mail addresses of all other members. This procedure facilitates a discussion involving research advice on specific technical challenges, which are permanently archived and searchable. Such exchanges can pose a serious threat to economic and technological security for two reasons. First, it is not uncommon for concepts, research, development, testing, and evaluation of a technology to take place in an open or unclassified environment. This is particularly significant when it comes to sensitive but unclassified or dual-use technologies and proprietary information. Second, a foreign national involved in collecting information on future programs or in acquiring research being conducted in another country could have an e-mail address from within the United States.

Avery Dennison: Target of Trade Secret Theft

In April 1999, two Taiwan executives and a Taiwan company were found guilty of violating Title 18 U.S.C. Section 1832 (Theft of Trade Secrets). Pin Yen Yang, president of Four Pillars Company, and his daughter Hwei Chen "Sally" Yang were accused of stealing adhesive formulas and innovations from Avery Dennison Corporation with the help of an Avery Dennison employee. This case marks the first conviction of foreign individuals or a foreign company that has gone to trial under the Economic Espionage Act.

On 5 January 2000, a Youngstown, Ohio, federal judge sentenced Pen Yen Yang to two years probation along with six months of home detention for violating the 1996 Economic Espionage Act. Mr. Yang's daughter was sentenced to one-year probation on the same charge. The Yangs each faced a maximum penalty of 10 years in prison and $250,000 in fines. Four Pillars, itself also was fined $5 million by a US District Court for accepting the pilfered secrets.

In February 2000, a jury verdict in US District Court, Cleveland awarded Avery Dennison at least $40 million in damages in a civil case against Four Pillars. The judge increased the award to $80 million.

Exploiting Multinational Conferences, Business Information Exchanges, or Joint Ventures. International technical and academic conferences, both home and abroad, offer an excellent venue for foreign collectors to obtain information and to spot and assess experts in a given field of interest. Many contractors involved with US Government and DoD contracts attend such conferences on behalf of their companies' commercial interests and thus can become targets of foreign collection. There have been many instances when US participants at international conferences have been contacted at a later date and asked to provide information on a given technology or proprietary data. Probing for information outside the scope of the conference is also a common activity. Often these approaches play on cultural commonalties as a reason to cooperate.

Misleading Open-Source Collection. Practitioners of economic and industrial espionage may employ legal, but misleading steps to hide a collector's true interest, affiliation, or location. For example, a collector may use public access Internet connections found at public libraries and educational institutions for browsing Web sites. This type of activity can protect the collector's identity and provide a means to "lose" the requester's individual inquiry amongst the multitude of requests generated from the public and educational computers. A public library presents a disarming persona, and the credibility of an educational institution inadvertently adds a measure of legitimacy to a request. Such misleading measures reduce the chance of a request raising suspicions and being reported to security personnel, while increasing the likelihood that a request will receive a response. Other misleading techniques include routing e-mail through one or more countries to hide the true point of origin and using contacts established through membership in professional organizations and at conference to unwittingly broker foreign visits or obtain the required information.

Illegal Collection

Acquisition of Export-Controlled Technologies. The unlawful acquisition of export-controlled technologies by foreign collectors is of growing concern. Methods of operation employed to circumvent the export-control process include: the use front companies within the United States and abroad, the illegal transportation of goods to an undisclosed end user by utilizing third country cut-outs or false end-user certificates, and the purchase of an exportable version of a product and then having it modified during the manufacturing process to meet the specifications of the export-controlled version. In 1999, for example, a US company reported that it received a telephone call from an individual in New York who wanted to purchase thousands of dollars worth of computer equipment, under a United Nations program, for shipment to Jordan. Several minutes into the conversation, the perspective buyer admitted that the computers were to be transshipped from Jordan to Iraq, an embargoed country.

Theft of Trade Secrets, Critical Technologies, and Critical Information. The theft of trade secrets, critical technologies, and critical information knows no boundaries. As recent cases indicate—from the insider threat, to laptop computer thefts, to hotel room intrusions abroad—foreign entities employ a wide range of redundant and complementary methods of operation. The perpetrators of economic and industrial espionage include traditional foreign intelligence services, state-sponsored educational and scientific institutions, and independent, nonstate-sponsored companies and individuals. The increased identification of nonstate sanctioned industrial espionage, however, should not be viewed as the demise of traditional foreign intelligence service clandestine espionage. US businessmen traveling abroad routinely report incidents of suspected targeting. Their briefcases and laptop computer have been tampered with, or outright stolen; they have reported excessive elicitation by foreign officials at border crossing points, and their hotel rooms have been searched.

Agent Recruitment, Co-optees, and US Volunteers. US persons with access to trade secrets, critical technologies, and classified information are potential recruits to aid in foreign collection operations. Some become unwitting facilitators by brokering foreign visits, the process of using a third party to arrange visits that circumvent official visitation procedures. In addition, foreign collectors have enticed US experts to present papers overseas as a means to exploit their knowledge of export-controlled information, or to facilitate their recruitment as agents or co-optees. Foreign intelligence services and other government-sponsored entities continue to employ traditional clandestine espionage methods to obtain US trade secrets, critical technologies, and critical information. These methods include agent recruitment, US volunteers, and co-optees.

Responding to the Challenge

National Counterintelligence Center

In a rapidly changing but still-hostile world, NACIC coordinates the US Government's effort to identify and counter foreign intelligence threats to US national and economic security. Operating under the auspices of the National Security Council, NACIC draws it staffing from counterintelligence and security professionals from the FBI, CIA DIA, NSA, the Office of the Secretary of Defense, the armed services, the Department of State, and DOE. In addition to producing the *Annual Report to Congress on Foreign Economic and Industrial Espionage*, NACIC's activities include a proactive industry outreach program. The NACIC outreach mission provides industry with threat awareness materials (literature, posters, videotapes, and briefings), and it sponsors regional awareness seminars and security fairs. For information on NACIC's activities and educational materials, visit the NACIC Internet Web site at http://www.nacic.gov.

Federal Bureau of Investigation

The FBI's public voice for espionage, counterintelligence, counterterrorism, as well as for economic espionage and cyber and physical infrastructure protection, and all national security issues is the Awareness of National Security Issues and Response Program (ANSIR)—this is the FBI's national security awareness program. ANSIR is designed to provide unclassified national security threat and warning information—specifically related to foreign-sponsored or foreign-coordinated intelligence—to US corporate security directors and executives, law enforcement, and other government agencies. The ANSIR program focuses on the "techniques of espionage," giving industry representatives tangible information to help them identify their own vulnerabilities. These techniques include the compromise of industry information through "dumpster diving" (searching through trash and discarded materials) where foreign intelligence services and competitors may try to obtain corporate proprietary information. They many also include listening devices that could be as simple as using a police scanner used to tune in the frequency of the wireless microphone being used in a corporate boardroom.

Each of the FBI's 56 field offices has an ANSIR coordinator who meets regularly with industry leaders and security directors for updates on current national security issues within their jurisdiction. Dissemination nationwide occurs through ANSIR e-mail and ANSIR fax networks. ANSIR fax was the first initiative by the US Government to provide 25,000 individual US corporations with critical technologies or sensitive economic information targeted by foreign intelligence services or their agents. ANSIR e-mail increased the capacity to over 100,000 recipients, which is expected to accommodate every US corporation that wishes to receive information from the FBI. Through the ANSIR program and the discussion of techniques of espionage, corporations are able to learn from the experiences of others enabling them to protect their commercial technologies.

For additional information concerning the FBI, visit its Internet Web site at http://www.fbi.gov. Information on the ANSIR Program can be obtained from the Web site http://www.fbi.gov/ansir/ansir.htm or sending an e-mail to ansir@leo.gov.

US Customs Service

The US Customs Service, as the principal law enforcement agency charged with enforcement of US international trade laws at its national borders, is the first line of defense in preventing illicit trafficking in strategic and controlled commodities, and in enforcing international economic sanctions and embargoes. It is the only border agency with an extensive air, land, and marine interdiction force and with an investigative component supported by its own intelligence branch. Illicit trafficking in weapons of mass destruction and their delivery systems, conventional weapons and firearms, dual-use technology, and stolen property and trade secrets pose serious threats to the United States, its economy, and its international partners. The US Customs Service's Internet Web site is http://www.customs.treas.gov.

US Department of Commerce, Bureau of Export Administration

The primary roles of the Bureau of Export Administration's (BXA) export enforcement program are to prevent the illegal export of dual-use items; investigate and assist in the prosecution of violators of the Export Administration Regulations (EAR) and the Fastener Quality Act (FQA); and inform and educate exporters, freight forwarders, and manufacturers of their enforcement responsibilities under the EAR and FQA. Export enforcement personnel also work closely with

the BXA's Office of Chief Counsel and the US Attorneys Offices in bringing enforcement actions against violators of the EAR. A list of denied persons contains information on the names and addresses of firms and individuals denied access to US goods, in addition to the reasons for the denial action. The BXA's Internet Wed site is http://www.bxa.doc.gov.

Overseas Security Advisory Council

The Department of State established the Overseas Security Advisory Council (OSAC) to foster the exchange of security-related information between the US Government and US private sector operating abroad. Administered by the Bureau of Diplomatic Security, OSAC has developed into a successful joint venture for security cooperation. OSAC maintains an Internet Web site that provides timely news items and travel warnings at http://www.ds-osac.org.

Department of Energy: Economic Espionage Threat Assessment

The DOE's Office of Counterintelligence (OCI) is currently engaged in a threat assessment on economic espionage with an emphasis on Cooperative Research and Development Agreements (CRADAs). CRADAs are agreements between one or more federal laboratories and one or more nonfederal parties under which the government, through its laboratories, provides personnel, facilities, or other resources with or without reimbursement. As an outcome of the threat assessment, OCI will make recommendations that will reduce the opportunities for economic espionage within the DOE.

Department of Defense

Within the DoD are agencies tasked with protecting technology and supporting cleared defense contractors. Cleared defense contractors are encouraged to contact the appropriate local representatives of these agencies: the Defense Security Service, the Air Force Office of Special Investigations, the Naval Criminal Investigative Service, and the Army Intelligence and Security Command.

Conclusion

As long as the United States remains the world's leading industrial power and US industry continues to lead the world in technology development, the United States will remain a prime target of foreign economic collection and industrial espionage. Indeed, economic collection against the United States, including the theft of trade secrets and competitive business information is likely to intensify in the new millennium as the race to control scarce resources and global markets intensifies. Not only have traditional allies and adversaries increased their economic collection activities against the United States, but as developing countries emerge as potential new economic competitors, they can be expected to increase their collection efforts against US targets, as well. Traditional allies as well as adversaries have increased and will continue to pursue economic collection activities against the United States.

Private industry and the counterintelligence community will continue to face the challenge of distinguishing legitimate competitive collection activities from those whose ultimate aims are the illegal transfer of trade secrets and critical technologies. It is the scrutiny of open-source collection that frequently reveals other illegal activities or intentions. Among economic collectors, malicious intentions may be more difficult to detect, but the increasing competition for limited global resources suggests that the problem will only increase.

Additional factors make the true extent of economic espionage difficult to measure. Successful espionage seldom comes to light, and even when economic espionage is discovered, companies are often reluctant to report to authorities that they have been the victim of such activity because of the embarrassing publicity and legal complications that may follow. The findings of a recent survey sponsored by PricewaterhouseCoopers indicate that Fortune 1,000 companies sustained losses in the billions in 1999 from the theft of their proprietary information. Some of the other key findings of this survey indicate:

- The greatest known losses to US companies involve information concerning the manufacturing processes and research and development.

- The global Internet and proliferation of information systems have significantly increased the risks to corporate proprietary information.

- On-site contract employees and original equipment manufacturers are now perceived as the greatest threat to proprietary information.

- The majority of companies have not effectively met the challenge of providing a framework for safeguarding proprietary information.

- Most companies lack a mechanism and process by which to assess the value of proprietary information.

The leading collectors of technical intelligence are most interested in the following information: classified US defense information—information systems, sensors and lasers, electronics, and aeronautic systems technologies—trade information, and commercial technologies. Collection efforts, either open-source or illegal collection are gradually increasing.

For Immediate Assistance

Here is who to contact if further assistance is required in the following:

- Industrial espionage: the local office of the FBI.
- Export violation: the local office of US Customs Service.
- Export control: the local office of the Department of Commerce, Bureau of Export Administration.

Reverse Blank

Appendix

Private Industry Survey

Officers of the National Counterintelligence Center contacted nearly a dozen selected Fortune 500 companies to obtain their views on the problem of foreign economic collection and industrial espionage. Following is a distillation of corporate responses to questions concerning their experience.

Is foreign economic information collection and/or industrial espionage a problem for your company or industry?

Yes. Each day America is driven more and more by information. Proprietary information is the chief competitive asset, vital to both our industry and our society. Our livelihood and our national strength depend on our ability to protect industrial and economic data. As the marketplace evolves and new technology is developed, information collectors are seeking competitive information we believe is intended to be used to gain competitive advantage over US corporations in several fields.

To what extent, if any, has your company and/or industry experienced aggressive economic information collection or industrial espionage by foreign entities?

Espionage can go on for years without a specific incident to trigger the situation; therefore, it is difficult to estimate the extent of economic information collection and/or industrial espionage by foreign entities. The economic resources of a potential enemy and their disposition offer it a selection of a range of possible or probable course of action. Suspicious activity—such as using excessive Xerox paper, reading technical manuals on a Saturday evening, wandering through restricted areas, and aggressively recruiting employees—has been observed.

What are the types of information or technology being targeted?

- Export-controlled information.
- Government programs.
- National Missile Defense.
- Unclassified and open-source information.
- Neurological technology.
- Leverage technology.
- Business plans.
- Pharmaceutical intellectual property.
- Formulas and research.
- Manufacturing process.
- Computer storage, memory, source codes, processors, and encryption.

What are the collection techniques employed?

Employees—not only disgruntled employees—contractors, consultants, and adversaries are viewed as great threats. Using today's technology, information can be downloaded into small disks and readily removed from the premises.

US companies' new initiative proprietary information tends to be contained in such an electronic format making it more vulnerable to economic espionage. Other collection techniques include:

- Breaking away from tour groups.
- Attempting access after normal working hours.
- Different personnel appear at the last minute.
- Theft of laptops.
- Customs holding laptops for a period of time.
- Requesting technical information.
- Social gatherings.
- Conferences and symposiums.
- Trade shows.
- Dumpster diving (searching through trash and discarded materials).
- Nonencrypted Internet messages.

Who are the most active collectors?

- China.
- Japan.
- Israel.
- France.
- Korea.
- Taiwan.
- India.

What initiative has your company or industry taken to counter foreign economic collection?

Senior business leaders, who have acknowledged that economic espionage is a real problem and it may affect the bottom line, have developed initiatives ranging from better control of physical security and access by foreign nationals—such as limited access—being in compliance with government contracts, and developing strong proprietary safeguards.

Although there is no absolute defense against covert attack, being alert to the possibility of danger and adherence to reasonable and prudent precautionary measures tend to reduce the threat. In this effort, businesses have developed security briefings, educational pamphlets, technical training, and on-line security information.

Are there any examples or case histories of aggressive foreign collection or industrial espionage you would be willing to share?

In August 1999, an employee of an aerospace engineering company approached the Security/Ethics Officer with a counterintelligence issue related to an overseas trip to China. The employee admitted that he had an outside business arrangement in the works with an individual from the West Coast. Under advisement from the FBI and US Customs Service he was asked to cooperate with his business associate. The technology at risk was a highly sensitive infrared camera, which can be used in missile guidance systems. The business associate was accused of violating the US Arms Export Control Act, which regulates defense articles (military weapons and munitions), defense services, and related technical data.

What should the US Government do to better support the private sector in countering this threat?

The US Government should foster the development of closer relations with the private sector, get to know the threat information needs of business, and help prevent companies inadvertently pairing up or doing business with those who are known to present a threat. Government must also do a better job of understanding and identifying what the United States must protect. In other words, identify the economic and technological "crown jewels" that we all must protect.

Industry security specialists find it difficult to convince their senior managers that the threat from foreign economic collection is a real and persistent one. This often means that the necessary resources to enhance protection and security are not allocated. They blame the government, in part, for not showing sufficient interest in their plight. To capture the attention of senior corporate managers and have them allocate sufficient resources into efforts enhancing security, the US Government should institute a more robust program to reach out to the business community, targeting senior corporate leadership with timely, credible, and specific information on the threat. Dated and anecdotal information will not do. To get buy-in from senior corporate management, government must be prepared to take some risks and share some relevant threat information in a timely manner. This has to be part of a continuing dialogue if there is to be partnership between government and the private sector.

Government must gain a better understanding of how businesses are run and the way businessmen think. There must also be a significant effort to better educate judges, prosecutors, and government investigators concerning business trends and techniques. This education would foster the development of new approaches to investigations, prosecution, and adjudication that are more responsive to the needs and limitations of business. Businesses find that economic espionage complaints, when handled in foreign counterintelligence investigative channels rather than criminal investigative ones, become immediately classified and, much to the frustration of the business involved, inaccessible.